

MENU

SEARCH

INDEX

DETAIL

JAPANESE

BACK

NEXT

2 / 4

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-175008  
 (43)Date of publication of application : 21.06.2002

(51)Int.Cl. G09C 1/00

(21)Application number : 2001-291419 (71)Applicant : NEC SOFT LTD  
 TSUJII SHIGEO  
 YDK:KK  
 MURATA MACH LTD  
 (22)Date of filing : 25.09.2001 (72)Inventor : TSUJII SHIGEO  
 MATSUOKA KENJI

(30)Priority

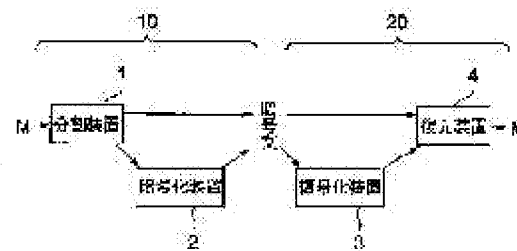
Priority number : 2000294435 Priority date : 27.09.2000 Priority country : JP

(54) ENCRYPTION METHOD, ENCRYPTION UNIT, AND ENCRYPTION AND DECODING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an encryption and decoding system enabling configuration of a speedy and easy cryptographic system.

SOLUTION: This encryption and decoding system is provided with an encryption unit, which has a dividing device 1 for dividing a plain text M into r-pieces of divided plaintexts (r is an integer larger than one); an encryption device 2 for ciphering n-pieces of the divided plain texts among the r-prices of divided plain texts ( $n < r$ ) into n-pieces of ciphertexts according to an arbitrary encryption method, and which outputs the remaining (r-n) pieces of divided plain texts and the n-pieces of ciphertexts as output ciphertexts; and a decoding unit 20 for receiving the output ciphertexts as in put ciphertexts, and the decoding unit 20 comprises a decoding device 3 for decoding the n-pieces of ciphertexts of the input ciphertexts into the n-pieces of divided plaintexts, and a restoring device 4 for restoring the plaintexts M from the remaining (r-n) pieces of divided plaintexts of the input ciphertexts and the n-pieces of divided plain texts from the decoding device 3.



## LEGAL STATUS

[Date of request for examination] 25.09.2001  
 [Date of sending the examiner's decision of rejection] 25.05.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-175008

(P2002-175008A)

(43) 公開日 平成14年6月21日 (2002.6.21)

(51) Int.Cl.<sup>7</sup>

G 0 9 C 1/00

識別記号

6 2 0

F I

G 0 9 C 1/00

テ-マ-ト\* (参考)

6 2 0 Z 5 J 1 0 4

審査請求 有 請求項の数11 O L (全 8 頁)

(21) 出願番号 特願2001-291419(P2001-291419)

(22) 出願日 平成13年9月25日(2001.9.25)

(31) 優先権主張番号 特願2000-294435(P2000-294435)

(32) 優先日 平成12年9月27日(2000.9.27)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000232092

エヌイーシーソフト株式会社

東京都江東区新木場一丁目18番6号

(71) 出願人 598159964

辻井 重男

東京都渋谷区神宮前四丁目2番19号

(71) 出願人 000139377

株式会社ワイ・デー・ケー

東京都稲城市押立1705番地

(74) 代理人 100071272

弁理士 後藤 祥介 (外1名)

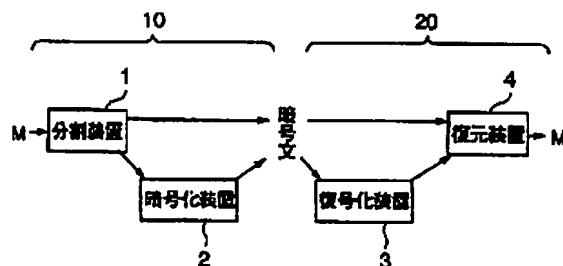
最終頁に続く

(54) 【発明の名称】 暗号化方法、暗号化器、暗号化及び復号化システム

(57) 【要約】

【課題】 高速で簡易な暗号系を構成できる暗号化及び復号化システムの提供。

【解決手段】 平文Mを $r$  ( $r$ は2以上の整数)個の分割平文に分割する分割装置1と、 $r$ 個の分割平文のうちの $n$ 個 ( $n < r$ )の分割平文を、任意の暗号化方式によって、 $n$ 個の暗号文に暗号化する暗号化装置2とを有し、残りの( $r-n$ )個の分割平文と $n$ 個の暗号文とを出力暗号文として出力する暗号化器10と、出力暗号文を入力暗号文として受ける復号化器20とを備えた暗号化及び復号化システムであって、復号化器20は、入力暗号文の $n$ 個の暗号文を $n$ 個の分割平文に復号化する復号化装置3と、入力暗号文の残りの( $r-n$ )個の分割平文と復号化装置3からの $n$ 個の分割平文とから、平文Mを復元する復元装置4とを有する。



## 【特許請求の範囲】

【請求項1】 平文Mを $r$  ( $r$ は2以上の整数)個の分割平文に分割するステップと、 $r$ 個の分割平文のうちの $n$ 個 ( $n < r$ )の分割平文を $n$ 個の暗号文に暗号化するステップと、残りの( $r-n$ )個の分割平文と前記 $n$ 個の暗号文とを出力暗号文として出力するステップとを含むことを特徴とする暗号化方法。

【請求項2】 平文Mを $r$  ( $r$ は2以上の整数)個の分割平文に分割する分割装置と、 $r$ 個の分割平文のうちの $n$ 個 ( $n < r$ )の分割平文を $n$ 個の暗号文に暗号化する暗号化装置とを有し、残りの( $r-n$ )個の分割平文と前記 $n$ 個の暗号文とを出力暗号文として出力することを特徴とする暗号化器。

【請求項3】 平文Mを $r$  ( $r$ は2以上の整数)個の分割平文に分割する分割装置と、 $r$ 個の分割平文のうちの $n$ 個 ( $n < r$ )の分割平文を、任意の暗号化方式によって、 $n$ 個の暗号文に暗号化する暗号化装置とを有し、残りの( $r-n$ )個の分割平文と前記 $n$ 個の暗号文とを出力暗号文として出力する暗号化器と；前記出力暗号文を入力暗号文として受ける復号化器と；を備えた暗号化及び復号化システムであって、前記復号化器は、前記入力暗号文の前記 $n$ 個の暗号文を前記 $n$ 個の分割平文に復号化する復号化装置と、前記入力暗号文の前記残りの( $r-n$ )個の分割平文と前記復号化装置からの前記 $n$ 個の分割平文とから、前記平文Mを復元する復元装置とを有することを特徴とする暗号化及び復号化システム。

【請求項4】 請求項3に記載の暗号化及び復号化システムにおいて、前記分割装置は、 $r$ 個の分割平文を $C_1, C_2, \dots, C_{(r-1)}, C_r$ とすると、どの2つをとってもお互いに公約数をもたない $r$ 個の自然数 $N_i$  ( $i=1, 2, \dots, r$ )を用いて、表わされる以下の式：

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$$\dots,$$

$$C_{(r-1)} = M \bmod N_{r-1},$$

$$C_r = M \bmod N_r,$$

に従って、平文Mを $r$ 個の分割平文 $C_1, C_2, \dots, C_{(r-1)}, C_r$ に分割することを特徴とする暗号化及び復号化システム。

【請求項5】 請求項4に記載の暗号化及び復号化システムにおいて、

前記 $r$ 個の自然数 $N_i$  ( $i=1, 2, \dots, r$ )の積Nを

$$N = N_1 \cdot N_2 \cdot \dots \cdot N_{r-1} \cdot N_r$$

とした時、平分Mを $\log_2 M \leq \log_2 N$ を満たす整数とし、

$N_r$ を法とする、任意の公開鍵暗号方式の暗号化関数 $E_r(\cdot)$ を公開鍵とし、

暗号化関数 $E_r(\cdot)$ に対する復号化関数 $D_r(\cdot)$ を秘密鍵と

することを特徴とする暗号化及び復号化システム。

【請求項6】 請求項5に記載の暗号化及び復号化システムにおいて、

前記暗号化装置は、 $Br = Er(Cr)$ によって、平分Mの一部である $Cr$ を $Br$ に暗号化し、

前記暗号化器は、 $C = (C_1, C_2, \dots, C_{(r-1)}, Br)$ を出力暗号文として出力することを特徴とする暗号化及び復号化システム。

【請求項7】 請求項6に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、 $Cr = Dr(Br)$ により $Cr$ を求め、

前記復元装置は、

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$$\dots,$$

$$C_{(r-1)} = M \bmod N_{r-1},$$

$$Cr = M \bmod N_r,$$

から、前記平分Mを復元することを特徴とする暗号化及び復号化システム。

【請求項8】 請求項6に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、 $Cr = Dr(Br)$ により $Cr$ を求め、

前記復元装置は、

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$$\dots,$$

$$C_{(r-1)} = M \bmod N_{r-1},$$

$$Cr = M \bmod N_r,$$

に中国人剰余定理(Chinese remainder theorem)を適用して、前記平分Mを復元することを特徴とする暗号化及び復号化システム。

【請求項9】 請求項3に記載の暗号化及び復号化システムにおいて、

前記分割装置は、平文Mを $r$ 個の平文 $U_1, U_2, \dots, U_r$ に分割すると共に、 $U_1, U_2, \dots, U_r$ をアダマール変換行列 $H(r, r)$ によって

$$H(r, r) \cdot (U_1, U_2, \dots, U_r) = (V_1, V_2, \dots, V_r)$$

と表わされる $V_1, V_2, \dots, V_r$ に変換し、 $V_1, V_2, \dots, V_r$ を前記 $r$ 個の分割平文として出力するものであることを特徴とする暗号化及び復号化システム。

【請求項10】 請求項9に記載の暗号化及び復号化システムにおいて、

前記暗号化装置は、 $V_r$ を法とする、任意の公開鍵暗号方式の暗号化関数 $E_r(\cdot)$ を公開鍵とし、 $Br = Er(V_r)$ によって、平分Mの一部である $V_r$ を $Br$ に暗号化し、

前記暗号化器は、 $V = (V_1, V_2, \dots, V_{(r-1)}, Br)$ を出力暗号文として出力することを特徴とする暗号化及び復号化システム。

【請求項11】 請求項10に記載の暗号化及び復号化システムにおいて、

前記復号化装置は、暗号化関数  $E_r(\ )$  に対する復号化関数  $D_r(\ )$  を秘密鍵とし、 $V_r = D_r(B_r)$  により  $V_r$  を求め、

前記復元装置は、 $V_1, V_2, \dots, V_{(r-1)}, V_r$  を、アダマール変換行列  $H(r, r)$  の逆行列  $H^{-1}(r, r)$  によって、 $H^{-1}(r, r) \cdot (V_1, V_2, \dots, V_r) = (U_1, U_2, \dots, U_r)$

と表わされる  $U_1, U_2, \dots, U_r$  に変換して、前記平文  $M$  を復元することを特徴とする暗号化及び復号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化方法、暗号化器、暗号化及び復号化システムに関し、特に公開鍵及び秘密鍵を用いて電子文書を暗号化及び復号化することにより、秘密通信を行う暗号化及び復号化システム（暗号情報変換装置）に関するものである。

【0002】

【従来の技術】従来の暗号化方法は、送信者と受信者との間に、暗号文の復号に用いる暗号情報を変換する変換部を有するセンタを設けて、送信者は、受信者を示す受信者情報と、送信する情報を暗号化した暗号文と、この暗号文の復元に用いる第1の暗号情報とをセンタに送信し、センタは、送信者から受信者情報、暗号文および第1の暗号情報をそれぞれ受信し、変換部により第1の暗号情報を受信者情報の示す受信者が復元可能な第2の暗号情報に変換し、この第2の暗号情報と暗号文とを受信者に送信し、受信者は、センタから第2の暗号情報と暗号文とを受信し、第2の暗号情報に基づいて暗号文を復号化することにより元の情報を得るようにしたものである。

【0003】さらに、暗号化及び復号化システム（暗号情報変換装置）は、自己の公開鍵を用いて暗号化された第1の暗号情報を入力する暗号情報入力部と、自己の秘密鍵を入力する装置秘密鍵入力部と、この自己の秘密鍵を用いて第1の暗号情報を復号化する復号部と、受信者の公開鍵を入力する受信者公開鍵入力部と、この受信者の公開鍵を用いて復号部からの出力を暗号化することにより第2の暗号情報を生成する暗号化部とを備えるものである。

【0004】

【発明が解決しようとする課題】従来の技術の問題点は、実用化されている公開鍵暗号の方式は、暗号化・復号処理に要する計算量が、共通鍵暗号に比較して桁違いに大きく、その結果、公開鍵暗号の用途は、主にデジタル署名、または、鍵配送に限られていることである。

【0005】それ故、本発明の目的は、高速で簡易な暗号系を構成できる暗号化方法、暗号化器、及び暗号化及び復号化システムを提供することにある。

【0006】本発明のもう一つの目的は、任意の安全な公開鍵暗号を構成要素として含む、高速で簡易なメタ暗号系を、中国人剰余定理をベースに構成する方法を提案

することである。

【0007】本発明の別の目的は、任意の安全な公開鍵暗号を構成要素として含む、高速で簡易なメタ暗号系を、アダマール変換をベースに構成する方法を提案することである。

【0008】

【課題を解決するための手段】本発明の第1の態様によれば、平文  $M$  を  $r$  ( $r$  は2以上の整数) 個の分割平文に分割するステップと、 $r$  個の分割平文のうちの  $n$  個 ( $n < r$ ) の分割平文を  $n$  個の暗号文に暗号化するステップと、残りの  $(r-n)$  個の分割平文と前記  $n$  個の暗号文とを出力暗号文として出力するステップとを含むことを特徴とする暗号化方法が得られる。

【0009】本発明の第2の態様によれば、平文  $M$  を  $r$  ( $r$  は2以上の整数) 個の分割平文に分割する分割装置と、 $r$  個の分割平文のうちの  $n$  個 ( $n < r$ ) の分割平文を  $n$  個の暗号文に暗号化する暗号化装置とを有し、残りの  $(r-n)$  個の分割平文と前記  $n$  個の暗号文とを出力暗号文として出力することを特徴とする暗号化器が得られる。

【0010】本発明の第3の態様によれば、平文  $M$  を  $r$  ( $r$  は2以上の整数) 個の分割平文に分割する分割装置と、 $r$  個の分割平文のうちの  $n$  個 ( $n < r$ ) の分割平文を、任意の暗号化方式によって、 $n$  個の暗号文に暗号化する暗号化装置とを有し、残りの  $(r-n)$  個の分割平文と前記  $n$  個の暗号文とを出力暗号文として出力する暗号化器と；前記出力暗号文を入力暗号文として受ける復号化器と；を備えた暗号化及び復号化システムであって、前記復号化器は、前記入力暗号文の前記  $n$  個の暗号文を前記  $n$  個の分割平文に復号化する復号化装置と、前記入力暗号文の前記残りの  $(r-n)$  個の分割平文と前記復号化装置からの前記  $n$  個の分割平文とから、前記平文  $M$  を復元する復元装置とを有することを特徴とする暗号化及び復号化システムが得られる。

【0011】本発明の第4の態様によれば、前述の第3の態様による暗号化及び復号化システムにおいて、前記分割装置は、 $r$  個の分割平文を  $C_1, C_2, \dots, C_{(r-1)}, C_r$  とすると、どの2つをとってもお互いに公約数をもたない  $r$  個の自然数  $N_i$  ( $i=1, 2, \dots, r$ )、すなわち、 $\gcd(N_i, N_j) = 1$  が  $N_i$  と  $N_j$  との最大公約数が1であることを表わすものとする、 $\gcd(N_i, N_j) = 1$  ( $i \neq j, i, j=1, 2, \dots, r$ ) を満たす  $r$  個の自然数  $N_i$  ( $i=1, 2, \dots, r$ )、を用いて、表わされる以下の式：

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$$\dots,$$

$$C_{(r-1)} = M \bmod N_{r-1},$$

$$C_r = M \bmod N_r$$

に従って、平文  $M$  を  $r$  個の分割平文  $C_1, C_2, \dots, C_{(r-1)}, C_r$  に分割することを特徴とする暗号化及び復号化シ

システムが得られる。

【0012】本発明の第5の態様によれば、前述の第4の態様による暗号化及び復号化システムにおいて、前記

$r$  個の自然数  $N_i$  ( $i=1, 2, \dots, r$ ) の積  $N$  を

$$N = N_1 \cdot N_2 \cdot \dots \cdot N_{r-1} \cdot N_r$$

とした時、平分  $M$  を  $\log_2 M \leq \log_2 N$  を満たす整数とし、 $N_r$  を法とする、任意の公開鍵暗号方式の暗号化関数  $E_r(\cdot)$  を公開鍵とし、暗号化関数  $E_r(\cdot)$  に対する復号化関数  $D_r(\cdot)$  を秘密鍵とすることを特徴とする暗号化及び復号化システムが得られる。

【0013】本発明の第6の態様によれば、前述の第5の態様による暗号化及び復号化システムにおいて、前記暗号化装置は、 $B_r = E_r(C_r)$  によって、平分  $M$  の一部である  $C_r$  を  $B_r$  に暗号化し、前記暗号化装置は、 $C = (C_1, C_2, \dots, C(r-1), B_r)$  を出力暗号文として出力することを特徴とする暗号化及び復号化システムが得られる。

【0014】本発明の第7の態様によれば、前述の第6の態様による暗号化及び復号化システムにおいて、前記復号化装置は、 $C_r = D_r(B_r)$  により  $C_r$  を求め、前記復元装置は、

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$\dots,$

$$C(r-1) = M \bmod N_{r-1},$$

$$C_r = M \bmod N_r$$

から、前記平分  $M$  を復元することを特徴とする暗号化及び復号化システムが得られる。

【0015】本発明の第8の態様によれば、前述の第6の態様による暗号化及び復号化システムにおいて、前記復号化装置は、 $C_r = D_r(B_r)$  により  $C_r$  を求め、前記復元装置は、

$$C_1 = M \bmod N_1,$$

$$C_2 = M \bmod N_2,$$

$\dots,$

$$C(r-1) = M \bmod N_{r-1},$$

$$C_r = M \bmod N_r$$

に中国人剰余定理(Chinese remainder theorem)を適用して、前記平分  $M$  を復元することを特徴とする暗号化及び復号化システムが得られる。

【0016】本発明の第9の態様によれば、前述の第3の態様による暗号化及び復号化システムにおいて、前記分割装置は、平文  $M$  を  $r$  個の平文  $U_1, U_2, \dots, U_r$  に分割すると共に、 $U_1, U_2, \dots, U_r$  をアダマル変換行列  $H(r, r)$  によって

$$H(r, r) \cdot (U_1, U_2, \dots, U_r) = (V_1, V_2, \dots, V_r)$$

と表わされる  $V_1, V_2, \dots, V_r$  に変換し、 $V_1, V_2, \dots, V_r$  を前記  $r$  個の分割平文として出力するものであることを特徴とする暗号化及び復号化システムが得られる。

【0017】本発明の第10の態様によれば、前述の第

9の態様による暗号化及び復号化システムにおいて、前記暗号化装置は、 $V_r$  を法とする、任意の公開鍵暗号方式の暗号化関数  $E_r(\cdot)$  を公開鍵とし、 $B_r = E_r(V_r)$  によって、平分  $M$  の一部である  $V_r$  を  $B_r$  に暗号化し、前記暗号化装置は、 $V = (V_1, V_2, \dots, V(r-1), B_r)$  を出力暗号文として出力することを特徴とする暗号化及び復号化システムが得られる。

【0018】本発明の第11の態様によれば、前述の第10の態様による暗号化及び復号化システムにおいて、前記復号化装置は、暗号化関数  $E_r(\cdot)$  に対する復号化関数  $D_r(\cdot)$  を秘密鍵とし、 $V_r = D_r(B_r)$  により  $V_r$  を求め、前記復元装置は、 $V_1, V_2, \dots, V(r-1), V_r$  を、アダマル変換行列  $H(r, r)$  の逆行列  $H^{-1}(r, r)$  によって、 $H^{-1}(r, r) \cdot (V_1, V_2, \dots, V_r) = (U_1, U_2, \dots, U_r)$  と表わされる  $U_1, U_2, \dots, U_r$  に変換して、前記平文  $M$  を復元することを特徴とする暗号化及び復号化システムが得られる。

【0019】

【発明の実施の形態】次に本発明について詳細に説明する。

【0020】本発明は、平分  $M$  を、 $C_1, C_2, \dots, C(r-1), C_r$  と  $r$  個に分割し、 $C_r$  だけは、任意の暗号化方式(暗号化関数  $E_r(\cdot)$ )によって、 $B_r = E_r(C_r)$  と暗号化し、 $C = (C_1, C_2, \dots, C(r-1), B_r)$  を暗号文とする。

【0021】この時、 $C$  より  $M$  が解読されることはない。

【0022】また、 $E_r(\cdot)$  に対する復号化関数  $D_r(\cdot)$  によって、 $C_r = D_r(B_r)$  を求め、前記平分  $M$  を復元する。

【0023】暗号化関数  $E_r(\cdot)$  を一方向性関数と仮定する。このとき、中国人の剰余定理(又はアダマル変換)により、 $(C_1, C_2, \dots, C(r-1), B_r)$  より  $M$  が得られることはない。

【0024】従って、完全解読されることはないという意味で、本方式は安全であることが証明される。 $M$  の情報の一部は、 $C_1, C_2, \dots, C(r-1)$  より、情報量的には、洩れていることになるが、具体的に平分の一部が明示的に解読されることはない。

【0025】また、 $r$  を大きくする程、平分  $M$  のビット当りの処置量は減少し高速になる。 $r$  は平分としての適正サイズ等を考慮して定められる。

【0026】次に、本発明の実施例について図面を参照して説明する。

【0027】図1を参照すると、本発明の第1の実施例による暗号化及び復号化システムは、暗号化器10と、復号化器20とを備えている。

【0028】暗号化器10は、平文  $M$  を  $r$  ( $r$  は2以上の整数) 個の分割平文に分割する分割装置1と、 $r$  個の分割平文のうちの  $n$  個 ( $n < r$ ) の分割平文を、任意の暗号化方式によって、 $n$  個の暗号文に暗号化する暗号化

装置2とを有し、残りの $(r-n)$ 個の分割平文と前記 $n$ 個の暗号文とを出力暗号文として出力する。

【0029】復号化装置20は、出力暗号文を入力暗号文として受ける。そして、復号化装置20は、入力暗号文の前記 $n$ 個の暗号文を前記 $n$ 個の分割平文に復号化する復号化装置3と、前記入力暗号文の前記残りの $(r-n)$ 個の分割平文と前記復号化装置からの前記 $n$ 個の分割平文とから、前記平文 $M$ を復元する復元装置4とを有する。

【0030】以下、暗号化装置10は、平文 $M$ を $r$ 個に分割し、そのうちの一つを任意の暗号化方式によって暗号化装置2で暗号化するものとして説明する。

【0031】暗号化装置10は、図2のように、分割装置1と、暗号化装置2とからなる。

【0032】分割装置1は、 $\gcd(N_i, N_j) = 1$  ( $i \neq j, i, j = 1, 2, \dots, r$ ) を満たす $r$ 個の自然数 $N_i$  ( $i = 1, 2, \dots, r$ ) の積 $N = N_1 \cdot N_2 \cdot \dots \cdot N_{r-1} \cdot N_r$  に対して、平文 $M$ を $\log_2 M \leq \log_2 N$  を満たす整数とし、

$$C1 = M \bmod N_1,$$

$$C2 = M \bmod N_2,$$

...

$$C(r-1) = M \bmod N_{r-1},$$

$$Cr = M \bmod N_r,$$

のように平文 $M$ を $r$ 個に分割する。

【0033】ただし、 $\gcd(N_i, N_j) = 1$  は、 $N_i$  と $N_j$  との最大公約数が1であることを意味する。なお、 $\gcd$ はGreatest Common Divisorの略である。

【0034】すなわち、 $\gcd(N_i, N_j) = 1$  ( $i \neq j, i, j = 1, 2, \dots, r$ ) を満たす $r$ 個の自然数 $N_i$  ( $i = 1, 2, \dots, r$ ) とは、どの2つをとってもお互いに公約数をもたない $r$ 個の自然数 $N_i$  ( $i = 1, 2, \dots, r$ ) ともいうことができる。

【0035】暗号化装置2は、 $N_r$ を法とする、任意の公開鍵暗号方式の暗号化関数 $E_r()$ を公開鍵とし、 $Br = E_r(Cr)$ によって、平文 $M$ の一部である $Cr$ を $Br$ に暗号化する。

【0036】最終的に、暗号化装置10は、 $C = (C1, C2, \dots, C(r-1), Br)$ を、暗号文として出力する。

【0037】復号化装置20は、図3のように、復号化装置3と、復元装置4とからなる。

【0038】復号化装置3は、暗号化関数 $E_r()$ に対する復号化関数 $Dr()$ を秘密鍵として、 $Cr = Dr(Br)$ により $Cr$ を復号化する。

【0039】復元装置4は、

$$C1 = M \bmod N_1,$$

\*

$$M = C1 \cdot n1 \cdot x1 + C2 \cdot n2 \cdot x2 + \dots + Cr \cdot nr \cdot xr \pmod{N}$$

$$= 2 \cdot 165 \cdot 2 + 1 \cdot 105 \cdot 2 + 4 \cdot 77 \cdot 8 \pmod{1155}$$

$$= 3334 \pmod{1155}$$

$$= 1024 \pmod{1155}$$

$$* C2 = M \bmod N_2,$$

...

$$C(r-1) = M \bmod N_{r-1},$$

$$Cr = M \bmod N_r,$$

に中国人剰余定理(Chinese remainder theorem)を適用して、平文 $M$ を復元する。中国人剰余定理は、中国では、孫子の剰余定理とも呼ばれている。中国人剰余定理を用いれば、 $C1 = M \bmod N_1, C2 = M \bmod N_2, \dots, Cr = M \bmod N_r$  から $M$ が一意に決まる。

【0040】次に、上述の第1の実施例の動作を説明する。

【0041】具体例として、 $r = 3$ の場合において、 $M = 1024$  を分割、暗号化し、復号化、復元する場合を説明する。

$$【0042】 N_1 = 7, N_2 = 11, N_3 = 15 (= 3 \cdot 5)$$

$$N = 7 \cdot 11 \cdot 15 = 1155$$

$$M = 1024 \text{ とする。}$$

$$【0043】$$

$$C1 = M \bmod N_1$$

$$20 \quad = 1024 \bmod 7 = 2 \bmod 7$$

$$C2 = M \bmod N_2$$

$$= 1024 \bmod 11 = 1 \bmod 11$$

$$C3 = M \bmod N_3$$

$$= 1024 \bmod 15 = 4 \bmod 15$$

$C3$ は任意の公開鍵暗号方式で暗号化する。

$$【0044】 B3 = E3(C3)$$

$C = (C1, C2, B3)$  を暗号文として送る。

【0045】 $B3$  を  $C3$  に復号化する。

$$【0046】 C3 = D3(B3)$$

$$30 \quad C1 = 2 \bmod 7$$

$$C2 = 1 \bmod 11$$

$$C3 = 4 \bmod 15$$

より中国人剰余定理を用いて  $M = 1024$  を復元する。

【0047】以下、中国人剰余定理の部分を説明する。

$$【0048】 n_i = N/N_i$$

ここでは

$$n1 = N/N_1$$

$$= 1155/7 = 165$$

$$n2 = N/N_2$$

$$40 \quad = 1155/11 = 105$$

$$n3 = N/N_3$$

$$= 1155/15 = 77$$

$$n_i \cdot x_i = 1 \bmod N_i$$

ここでは

$$x1 = 2, x2 = 2, x3 = 8$$

より  $M = 1024$  を得る。

【0049】次に、本発明の第2の実施例による暗号化及び復号化システムについて説明する。

【0050】この暗号化及び復号化システムは、図4に示した暗号化装置10'と、図5に示した復号化装置20'とを備えている。

【0051】図4において、暗号化装置10'は、平文Mを $r$  ( $r$ は2以上の整数)個の分割平文に分割する分割装置1'と、 $r$ 個の分割平文のうちの $n$ 個 ( $n < r$ )の分割平文を、任意の暗号化方式によって、 $n$ 個の暗号文に暗号化する暗号化装置2'とを有し、残りの( $r - n$ )個の分割平文と前記 $n$ 個の暗号文とを出力暗号文として出力する。

【0052】図5において、復号化装置20'は、出力暗号文を入力暗号文として受ける。そして、復号化装置20'は、入力暗号文の前記 $n$ 個の暗号文を前記 $n$ 個の分割平文に復号化する復号化装置3'と、前記入力暗号文の前記残りの( $r - n$ )個の分割平文と前記復号化装置からの前記 $n$ 個の分割平文とから、前記平文Mを復元する復元装置4'とを有する。

【0053】以下、暗号化装置10'は、平文Mを $r$ 個に分割し、そのうちの一つを任意の暗号化方式によって暗号化装置2'で暗号化するものとして説明する。

【0054】図4において、暗号化装置10'は、分割装置1'と、暗号化装置2'とからなる。

【0055】分割装置1'は、平文Mを、 $r$ 個の平文 $U_1, U_2, \dots, U_r$ に分割すると共に、 $U_1, U_2, \dots, U_r$ をアダマール変換行列 $H(r, r)$ によって $H(r, r) \cdot (U_1, U_2, \dots, U_r) = (V_1, V_2, \dots, V_r)$ と表わされる $V_1, V_2, \dots, V_r$ に変換し、 $V_1, V_2, \dots, V_r$ を $r$ 個の分割平文として出力する。

【0056】暗号化装置2'は、 $V_r$ を法とする、任意の公開鍵暗号方式の暗号化関数 $E_r()$ を公開鍵とし、 $Br = E_r(V_r)$ によって、平文Mの一部である $V_r$ を暗号化する。

【0057】最終的に、暗号化装置10'は、 $V = (V_1, V_2, \dots, V(r-1), Br)$ を、出力暗号文として出力する。

【0058】図5において、復号化装置3'は、暗号化関数 $E_r()$ に対する復号化関数 $Dr()$ を秘密鍵として、 $V_r = Dr(Br)$ により $V_r$ を求める。

$$\begin{aligned} H^{-1}(r, r) \cdot (V_1, V_2, V_3, V_4) &= H^{-1}(4, 4) \cdot (10, -2, 0, -4) \\ &= (1, 2, 3, 4) \\ &= (U_1, U_2, U_3, U_4) \end{aligned}$$

より、 $M=1234$ を得る。

【0071】

【発明の効果】以上説明したように、本発明による第1の効果は、安全性である。

【0072】平文Mは、 $Nr$  (又は $V_r$ )だけの不確定さで、復号者以外に秘匿される。

【0073】また、実際には、 $E_r()$ の完全な一方向性

\*【0059】復元装置4'は、 $V_1, V_2, \dots, V(r-1), V_r$ を、アダマール変換行列 $H(r, r)$ の逆行列 $H^{-1}(r, r)$ によって、

$$H^{-1}(r, r) \cdot (V_1, V_2, \dots, V_r) = (U_1, U_2, \dots, U_r)$$

と表わされる $U_1, U_2, \dots, U_r$ に変換して、前記平文Mを復元する。

【0060】次に、上述の第2の実施例の動作を説明する。

【0061】具体例を、 $r = 4$ として、 $M=1234$ を分割、暗号化し、復号化、復元する。

【0062】 $U_1=1, U_2=2, U_3=3, U_4=4$ と分割する。

【0063】アダマール変換行列 $H(r, r)$ によって、 $H(r, r) \cdot (U_1, U_2, U_3, U_4) = (V_1, V_2, V_3, V_4)$ と変換する。

【0064】 $r = 4$ であるから、アダマール変換行列 $H(r, r)$ は

$$H(4, 4) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

である。

20 【0065】

$$\begin{aligned} H(r, r) \cdot (U_1, U_2, U_3, U_4) &= H(4, 4) \cdot (1, 2, 3, 4) \\ &= (10, -2, 0, -4) \\ &= (V_1, V_2, V_3, V_4) \end{aligned}$$

$V_4=-4$ は任意の公開鍵暗号方式で暗号化する。

【0066】 $B_4 = E_4(-4)$

$$V = (V_1, V_2, V_3, B_4)$$

$= (10, -2, 0, B_4)$ を暗号文として送る。

【0067】 $B_4$ を $V_4$ に復号化する。

【0068】

$$30 \quad V_4 = D_4(B_4)$$

$$= -4$$

アダマール変換行列 $H(4, 4)$ の逆行列 $H^{-1}(4, 4)$ によって、

$$H^{-1}(4, 4) \cdot (V_1, V_2, V_3, V_4) = (U_1, U_2, U_3, U_4)$$

と変換する。

【0069】 $r=4$ であるから、逆行列 $H^{-1}(4, 4)$ は

$$H^{-1}(4, 4) = (1/4) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

【0070】

\*40

$$\begin{aligned} H^{-1}(r, r) \cdot (V_1, V_2, V_3, V_4) &= H^{-1}(4, 4) \cdot (10, -2, 0, -4) \\ &= (1, 2, 3, 4) \\ &= (U_1, U_2, U_3, U_4) \end{aligned}$$

は保証されないもので、例えば、RSA(Rivest-Shamir-Adleman)暗号と楕円エルガマル暗号等、2種類以上の公開鍵暗号方式を、複雑さと処理速度とのトレードオフを考慮しつつ、併用することも考えられる。

【0074】本発明による第2の効果は、高速性である。

50 【0075】 $r=10$ とすると、暗号化・復号処理速度は1



0倍近く向上するものと期待される。

【図面の簡単な説明】

【図1】本発明の第1の実施例による暗号化及び復号化システムのブロック図である。

【図2】図1の暗号化及び復号化システムにおける暗号化器10のブロック図である。

【図3】図1の暗号化及び復号化システムにおける復号化器20のブロック図である。

【図4】本発明の第2の実施例による暗号化及び復号化システムにおける暗号化器10'のブロック図である。

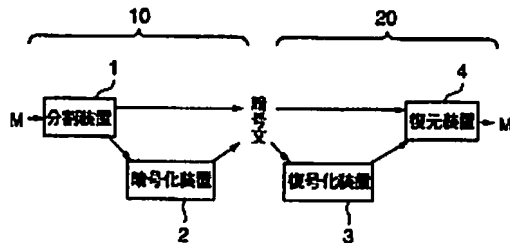
【図5】前述の第2の実施例による暗号化及び復号化システムにおける復号化器20'のブロック図である。

【符号の説明】

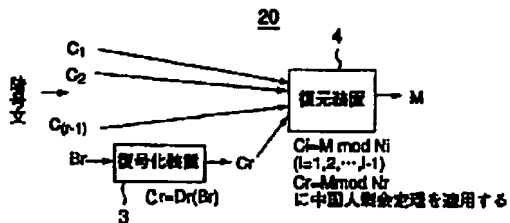
\*

- \* 1 分割装置
- 2 暗号化装置
- 3 復号化装置
- 4 復元装置
- 10 暗号化器
- 20 復号化器
- 1' 分割装置
- 2' 暗号化装置
- 3' 復号化装置
- 4' 復元装置
- 10' 暗号化器
- 20' 復号化器

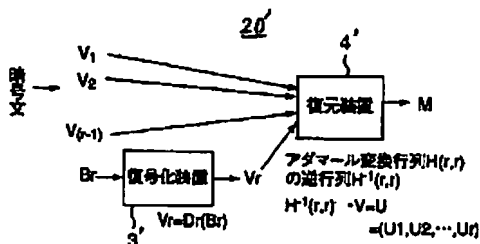
【図1】



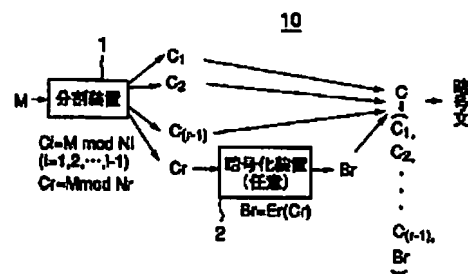
【図3】



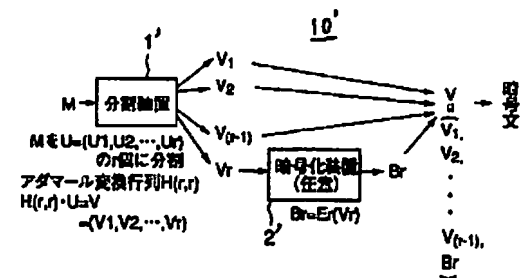
【図5】



【図2】



【図4】



## フロントページの続き

(71)出願人 000006297  
村田機械株式会社  
京都府京都市南区吉祥院南落合町3番地  
(72)発明者 辻井 重男  
東京都渋谷区神宮前四丁目2番19号

(72)発明者 松岡 賢志  
東京都江東区新木場一丁目18番6号 エヌ  
イーシーソフト株式会社内  
Fターム(参考) 5J104 AA18 JA26 NA02